UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/606,659	06/25/2003	Bing Wang	08212/0200290-US0/NC28834	4744

53666 7590 02/26/2008

BRAKE HUGHES BELLERMANN LLP
c/o INTELLEVATE
P.O. BOX 52050
MINNEAPOLIS, MN 55402

EXAMINER	
LASHLEY, LAUREL L	

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
02/26/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/606,659	WANG ET AL.	
	Examiner	Art Unit	
	LAUREL LASHLEY	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 November 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,4-6,8-10,12,14-17,19,21,22,24,25 and 30-43* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,4-6,8-10,12,14-17,19,21,22,24,25 and 30-43* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 11/21/2007 has been entered. Claims 1, 4-6, 8-10, 12, 14-17, 19, 21-22, 24-25 and 30-43 are pending.

Claim Objections

2. Claim 1 is objected to because of the following informalities: recitation of "an/the object", then a later recitation of "objects". Appropriate correction is required.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3. Claims 12, 14-17, 19, 21-22, 24-25, 34-35, and 39-42 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Independent claims 12 and 17 recite computer readable mediums, which according to Applicant's disclosure (see page 11, lines 12-24) includes data signals and/or carrier waves, which are not within any of the four statutory categories of invention.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 1,4-6, 8-10, 12,14-17, 9, 21-22, 24-25 and 30-43 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

5. Claims 1, 19, and 30 (and associated independent claims) recite the limitation "a second set of {hash values}" where there is no previous disclosure of a preceding (i.e. first) set of {hash values}. Similarly, Claims 1 recites “a third {hash value}” and “a fourth set of {hash values}”, again where there is no previous disclosure of a preceding (i.e. second) {hash value} and (i.e. third) set of {hash values}. There is insufficient antecedent basis for this limitation in the claim.

6. Claims 4, 5, 14, 15, 21, 24, 36 and new claims 37-43 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential elements, such omission amounting to a gap between the elements. See MPEP § 2172.01 as it relates to 35 USC 112, second paragraph. The omitted elements are the steps required to calculate or compute a “rough outline {hash value}” and a “sophisticated signature {hash value}”.

The Applicant has recited these two limitations in claims 4 and 5, respectively. However neither an “ROHV” nor a “SSHV” is a conventional term of art. Because of this, one of ordinary skill in the art of computer science would not know how to produce these two computations or values without details disclosing their essential elements and the steps required to produce them.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1, 6, 8-10,12, 14-17, 19, 21-22, 24-25 and 30-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chen et al. in US Patent No. 5960170 and further in view of Touboul in US Patent No. 6804780.

In reference to claim 1 and 36:

Chen et al. (Column 12, line 35 – Column 14, line 67) & (Figure 2) discloses a method for filtering out exploits passing through a device, comprising:

- Receiving an object directed to the device, where the object directed to the device is the virus scanning object, and where the device is the client. (Column 6, line 15-26)
- Determining a first {hash value} associated with the object, where the first {hash value} associated with the object is string A1 for virus A. (Column 13, line 24 – 37)
- Determining a second set of {hash values} associated with objects that have previously been scanned, where the second set of {hash values} are the set of virus strings: A1, A2, and A3, where the second set of {hash values} are the set of virus strings comprising virus string A which is associated with virus A (Figure 4d, 4b) and the set of virus strings have been previous scanned to determine that they are apart of the virus. (Column 13, line 1-37)
- If the first {hash value} matches at least one of the {hash values} in the second set, where a determination is made if the first {hash value} A1, matches one of the {hash values} in the second set. (Column 13, line 57 – Column 14, line 31)
- Determining a third {hash value} associated with the object, where the third {hash value} is virus string B1. (Column 13, line 24 – 37)
- Determining a fourth set of {hash values} associated with the objects that have previously been scanned, where the fourth set of {hash values} are the set of virus strings: B1, B2, and B3, where the fourth set of {hash values} are the set of virus strings

comprising virus string B which is associated with virus B (Figure 4d, 4b) and the set of virus strings have been previous scanned to determine that they are apart of the virus. (Column 13, line 1-37)

- If the third {hash value} matches at least one of the {hash values} in the fourth set, immediately processing the object, where if the third {hash value} B1 matches one of the {hash values} in the set of B virus strings, the object is processed by producing an additional virus detection object. (Column 13, line 57 – Column 14, line 31) *but does not expressly disclose hash value(s).*

Touboul however does disclose hash values (Column 2, lines 12-16; Figure 8).

Chen et al. and Touboul are analogous art because they are from similar problem solving areas (detecting and protecting computers from hostile viruses or codes). At the time of the invention it would have been obvious to modify the detection system of Chen et al. to incorporate verifying hash values as taught by Touboul as this is a well-known method in the art for virus or hostile code detection.

In reference to claim 6:

Chen et al. (Column 12, line 35 – Column 14, line 67) & (Figure 2) discloses the method of claim 1, wherein immediately processing the object further comprises forwarding the object to an output component without scanning the object, where the object is not scanned for virus C or any viruses who signatures portions being searched for were not found.

In reference to claim 8:

Chen et al. (Column 12, lines 35-54) & (Column 13, line 1 – Column 14, line 25) & (Figure 2) discloses the method of claim 6, wherein immediately processing the object further comprises

forwarding the object to a destination, where the object is forwarded to the server to determine if a second virus detection object needs to be transmitted.

In reference to claim 9:

Chen et al. (Column 12, line 35 – Column 14, line 67) & (Figure 2) discloses the method of claim 1, further comprising if the first {hash value} does not match any of the {hash values} in the second set,

- Scanning the object for an exploit, where the object is scanned for a virus exploit.
- Updating the second set of {hash values} to include the first {hash value}, where the second set of {hash values} A1, A2, A3, includes the first {hash value} A1. (Column 13, lines 24 – line 67)

In reference to claim 10:

Chen et al. (Column 12, line 35 – Column 14, line 67) & (Figure 2) discloses the method of claim 1, further comprising if the third {hash value} does not match any of the {hash values} in the fourth set,

Scanning the object for an exploit, where the object is scanned for a virus exploit

- Updating the fourth set of {hash values} to include the third {hash value}, where the fourth set of {hash values} B1, B2, B3, includes the third {hash value} B1. (Column 13, lines 24 – line 67)

In reference to claim 12:

Chen et al. (Column 12, line 35 – Column 14, line 67) & (Figure 2) & (Figure 4d) discloses the computer readable medium encoded with a data-structure, comprising:

- A first indexing data field having indexing entries, each indexing entry including a first {hash value}, where the first indexing entry includes the value of the virus sub-signatures. (Figure 4d)
- A second data field including object-related entries, each object-related entry having a second value and being indexed to an indexing entry in the first indexing data field, each object-related entry being uniquely associated with an object that has been previously scanned, where the second data fields comprise the composite virus signatures, and each virus object related entry is uniquely associated with the virus it identifies, and where these signatures were previously determined or "scanned" to match it with the virus it identifies (Figure 4d), *but does not expressly disclose hash value(s).*

Touboul however does disclose hash values (Column 2, lines 12-16; Figure 8).

Chen et al. and Touboul are analogous art because they are from similar problem solving areas (detecting and protecting computers from hostile viruses or codes). At the time of the invention it would have been obvious to modify the detection system of Chen et al. to incorporate verifying hash values as taught by Touboul as this is a well-known method in the art for virus or hostile code detection.

In reference to claim 16:

Chen et al. (Column 12, line 35 – Column 14, line 67) & (Figure 2) & (Figure 4d) discloses the computer-readable medium of claim 12, wherein at least one object-related entry in the second data field includes information about the associated object, where the data in second data field includes signature information to identify a virus.

In reference to claim 17:

Chen et al. discloses a system embodied on a computer-readable medium encoded with a data-structure for protecting a device against an exploit, comprising:

- A message tracker that is configured to determined whether an object has been previously scanned using a two-phase {hash value} technique, where the message tracker tracks down the virus detection object that is sent from the server to the client. (Column 6, lines 15-26), and where a determination is made to see if the object has been previously scanned using an iterative virus string detection technique. (Column 14, lines 13-63), and where the two phase {hash value} technique comprises the iterations of the virus signature string detection, and the determination of previously scanned necessarily occurs in the determination of whether another virus detection object need to be made and additional scanning is needed. (Figure 2, Item 245)
- A scanner component that is coupled to the message tracker and that is configured to receive an unscanned object and to determine whether the unscanned object includes an exploit, where the scanner component is coupled to the iterative virus detection module (Figure 4b), *but does not expressly disclose hash value(s).*

Touboul however does disclose hash values (Column 2, lines 12-16; Figure 8).

Chen et al. and Touboul are analogous art because they are from similar problem solving areas (detecting and protecting computers from hostile viruses or codes). At the time of the invention it would have been obvious to modify the detection system of Chen et al. to incorporate verifying hash values as taught by Touboul as this is a well-known method in the art for virus or hostile code detection.

In reference to claim 19:

Chen et al. (Column 12, lines 35-54) & (Column 13, line 1 – Column 14, line 25) & in particular (Column 13, line 24-37) discloses the system of claim 17, wherein the two-phase {hash value} technique comprises:

- Determining a first {hash value} associated with the object, where the first {hash value} associated with the object is string A1 for virus A. (Column 13, line 24 – 37)
- Determining a second set of {hash values} associated with objects that have previously been scanned, where the second set of {hash values} are the set of virus strings: A1, A2, and A3, where the second set of {hash values} are the set of virus strings comprising virus string A which is associated with virus A (Figure 4d, 4b) and the set of virus strings have been previous scanned to determine that they are apart of the virus. (Column 13, line 1-37)
- If the first {hash value} does not match at least one of the {hash values} in the second set, determining that the object has not been previously scanned, where a determination is made if the first {hash value} A1, matches one of the {hash values} in the second set. (Column 13, line 57 – Column 14, line 31)

In reference to claim 22:

Chen et al. (Column 12, lines 35-54) & (Column 13, line 1 – Column 14, line 25) & in particular (Column 13, line 24-37) discloses the system of claim 19, wherein the two-phase {hash value} technique further comprises:

If the first {hash value} matches at least one of the {hash values} in the second set,

- Determining a third {hash value} associated with the object, where the third {hash value} is virus string B1. (Column 13, line 24 – 37)

- Determining a fourth set of {hash values} associated with the objects that have previously been scanned, where the fourth set of {hash values} are the set of virus strings: B1, B2, and B3, where the fourth set of {hash values} are the set of virus strings comprising virus string B which is associated with virus B (Figure 4d, 4b) and the set of virus strings have been previous scanned to determine that they are apart of the virus. (Column 13, line 1-37)
- If the third {hash value} does not match at least one of the {hash values} in the fourth set, determining that the object has not been previously scanned, where if the third {hash value} B1 matches one the {hash values} in the set of B virus strings, the object is processed for viruses. (Column 13, line 57 – Column 14, line 31)

In reference to claim 25:

Chen et al. (Column 12, line 35 – Column 14, line 67) & (Figure 2) discloses the system of claim 22, wherein the two-phase {hash value} technique further comprises:

- If the third {hash value} approximately matches at least one of the {hash values} in the fourth set, determining that the object has been previously scanned, where if string B1 matches one of the {hash values} in the B set of strings, it can be determined that the object has been previously scanned in that a determination has also been made to see if the object has virus string A or virus string C within it. (Column 13, line 55 – Column 14, line 30)

In reference to claim 30:

Chen et al. discloses the method of claim 1, wherein:

- the first {hash value} and third {hash value} are determined by the device; (Column 13, lines 24 – 37) and
- the second set of {hash values} and the fourth set of {hash values} are determined by the device based on previous scanning by the device (Column 13, lines 1 – 37).

In reference to claim 31 and similar claim 34:

Chen et al. (Column 5, lines 34 – 45) discloses the method of claim 1, wherein the method is performed by a firewall.

In reference to claim 32 and similar claim 35:

Chen et al. (Column 5, lines 34 – 45) discloses the method of claim 1, wherein the method is performed by a router.

In reference to claim 33:

Chen et al. (Column 15, lines 5-13) discloses the method of claim 1, further comprising:
determining whether the object is compressed; and
if the object is compressed, decompressing the object.

In reference to claim 37, 39 and 41:

Chen et al. (Column 13, lines 27-31: virus signature…broken pieces) discloses wherein the determining the first {hash value} includes determining a rough outline {hash value} (ROHV) based on a {hash value} of a first portion of the object.

In reference to claim 38, 40 and 42:

Chen et al. (Column 13, lines 34-37) discloses wherein determining the third {hash value} includes determining a sophisticated signature {hash value} (SSHV) based on a Message Digest -5, a Secure Hash Algorithm, or a Secure Hash Standard, and wherein the ROHV requires less time to compute than the SSHV.

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Moran in US Patent No. 7032114 discloses a system and method for using signatures to detect computer intrusions.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to LAUREL LASHLEY whose telephone number is (571)272-0693. The examiner can normally be reached on Monday - Thursday, alt Fridays btw 7:30 am & 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, Jr. can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Laurel Lashley /Benjamin E Lanier/

Examiner
Art Unit 2132

Primary Examiner, Art Unit 2132

/L. L./
13 February 2008